Tweede Kamer der Staten-Generaal 2

Vergaderjaar 2015–2016

33 842 Evaluatie Wet politiegegevens en Wet justitiële en strafvorderlijke gegevens

Nr. 3 BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 7 december 2015

Met deze brief wil ik u informeren over de uitkomsten van de privacy-audit die de Auditdienst Rijk (ADR) heeft verricht naar de naleving van de Wet politiegegevens (Wpg) door de politie. De korpschef moet op grond van de Wpg ten minste vierjaarlijks een externe privacy-audit laten verrichten. Het auditrapport is eerder deze week aangeboden aan het College bescherming persoonsgegevens (CBP). Ik bied het rapport hierbij aan uw Kamer aan[1].

Daarnaast wil ik u informeren over de uitkomsten van het onderzoek van het CBP naar de naleving door de politie in Nederland van informatiebeveiligings- en gegevensbeschermingsvoorschriften van het Schengen Informatiesysteem (N.SIS-II) en het auditrapport van de ADR naar de beveiliging van het Europees Visum Informatiesysteem (EUVIS).

Uit de privacy-audit naar de naleving van de Wpg blijkt dat de politie op essentiële punten nog onvoldoende aan de wet voldoet. Ook met betrekking tot het N.SIS-II en het EUVIS tonen de onderzoeken tekortkomingen in de naleving door de politie. Het beeld dat uit deze rapportages naar voren komt, baart mij vanzelfsprekend zorgen.

Ik acht het van groot belang dat de politie deze regels nauwgezet naleeft. De samenleving is niet alleen gebaat bij een goede taakuitvoering door de politie, maar ook bij een zorgvuldige omgang met politiegegevens die voor die taakuitvoering noodzakelijk is. Veiligheid en het respecteren van de privacy zijn onlosmakelijk met elkaar verbonden.

Ook de korpschef is ervan doordrongen dat de politie deze wetgeving structureel goed moet naleven. Een aantal maatregelen is daarvoor al in gang gezet. Aanvullende maatregelen zullen door de korpschef worden

[1] Raadpleegbaar via www.tweedekamer.nl

kst-33842-3
ISSN 0921 - 7371
's-Gravenhage 2015

uitgewerkt in een wettelijk voorgeschreven verbeterplan, dat uiterlijk 1 maart 2016 gereed moet zijn en waarvan ik van de korpschef verwacht dat het realistisch haalbaar is, met een ambitieus perspectief voor de toekomst. Ik heb met de korpschef afspraken gemaakt over de criteria waaraan het verbeterplan minimaal moet voldoen. Deze afspraken zal ik verderop in mijn brief toelichten.

Algemeen

Een belangrijk fundament in onze rechtsstaat is de bescherming van de persoonlijke levenssfeer van onze inwoners. Iedereen heeft recht op persoonlijke vrijheid en individuele autonomie. Onderdeel van dit recht is de bescherming van een ieders persoonsgegevens. De politie is voor onze veiligheid in grote mate afhankelijk van de beschikbaarheid van informatie en moet daartoe effectief en efficiënt persoonsgegevens kunnen verwerken.

De Wpg geeft invulling aan het besef dat het verwerken van persoonsgegevens door de politie in het kader van de veiligheid een grote verantwoordelijkheid met zich meebrengt. Burgers moeten erop kunnen vertrouwen dat de politie correct en zorgvuldig met persoonsgegevens omgaat. Een goede naleving van de Wpg leidt tot een evenwicht waarin de politie voldoende middelen ter beschikking staan om te werken aan de veiligheid van onze samenleving, zonder daarbij onnodig een inbreuk te maken op de grondrechten van burgers. Ik vind het van groot belang dat de politie de regels uit deze wet nauwgezet naleeft.

Privacy-audit Wpg

Op basis van eerdere audits en de evaluatie van de Wpg uit 2013[2] was al duidelijk geworden dat de Wpg, de politiepraktijk en de huidige ICT ondersteuning niet goed op elkaar aansluiten. In de evaluatie werd dit gekenmerkt als een «worstelende praktijk», waarbij de onderzoekers overigens niet was gebleken van klachten die wijzen op een systematische aantasting van de persoonlijke levenssfeer. In de nu voorliggende auditrapportage wordt het beeld van een worstelende praktijk opnieuw bevestigd. De politie voldoet op vijf essentiële thema's – autoriseren, verstrekken, protocolleren, bewaartermijnen en rechten van betrokkene – nog onvoldoende aan de wet. Dit baart mij zorgen.

Achtergrond

De Wpg is op 1 januari 2008 in werking getreden, ten tijde van het regionale politiebestel. Voor een goede naleving van de Wpg moeten de juiste organisatorische en technische randvoorwaarden worden gecreëerd. Een voorbeeld hiervan is het zodanig inrichten van de ICT-systemen dat het geautomatiseerd verwijderen en vernietigen van gegevens mogelijk wordt gemaakt. In het oude politiebestel is het onvoldoende gelukt om de technische randvoorwaarden te realiseren. Ook op organisatorisch vlak is een aantal maatregelen onvoldoende uitgewerkt, waaronder een procedure voor het intrekken van autorisaties.

Met het inwerkingtreden van de Politiewet 2012 is vanaf 2013 het voeren van centrale regie op de naleving van de Wpg mogelijk geworden. Hiermee is een belangrijke voorwaarde gecreëerd om fundamentele stappen te zetten om de naleving van de Wpg op orde te brengen. De politie heeft vanaf 2013 diverse maatregelen getroffen, zoals de oprichting van de interne Gegevensautoriteit, het uniform beschrijven van diverse

[2] Kamerstuk 33 842, nrs. 1 en 2

werkprocessen, het introduceren van *privacy by design* voor vernieuwingen en wijzigingen in de informatievoorziening en vele bewustwordingssessies onder het politiepersoneel.

De nieuwe mogelijkheden van centrale sturing zijn, ondanks de vele inspanningen om de Wpg goed te implementeren en na te leven, nog onvoldoende benut.

Bovendien bleek uit de evaluatie van de Wpg dat de wet op bepaalde onderdelen te complex is. Ik heb daarom aangekondigd om de Wpg en de eveneens geëvalueerde Wet justitiële en strafvorderlijke gegevens in onderlinge samenhang te zullen herzien. Deze herziening heeft ten doel de complexiteit van beide wetten voor de uitvoeringspraktijk terug te dringen en de toepasbaarheid ervan in de keten te vergroten. Die herziening kan echter op dit moment nog niet plaatsvinden. Dit houdt verband met de lopende onderhandelingen in Brussel over een nieuwe algemene verordening gegevensbescherming en een nieuwe richtlijn gegevensbescherming voor het politie- en justitiedomein. De herziening zal moeten aansluiten bij deze ontwikkelingen in EU-verband. Een tussentijdse wetswijziging acht ik onwenselijk, omdat daarmee de uitvoeringspraktijk in korte tijd twee keer zou worden belast met wijzigingen in deze complexe wetgeving.
Wel richt ik mij op de voorbereidingen van het wetgevingstraject, nu de triloogbesprekingen over het Europees gegevensbeschermingspakket op intensieve wijze plaatsvinden.

Samenvatting bevindingen ADR

De centrale vraagstelling voor deze privacy-audit was in welke mate de politie in de periode 2011 tot en met 2014 heeft voldaan aan de bepalingen uit de Wpg. In samenspraak met het CBP richt deze audit zich op vijf hoofdthema's waarvan bekend was dat deze onvoldoende waren geïmplementeerd en waarvan het onvoldoende naleven de grootste impact heeft op de persoonlijke levenssfeer. Op zeven andere onderwerpen uit de Wpg heeft een lichtere vorm van toetsing plaatsgevonden. De algemene conclusie luidt dat de politie onvoldoende aan de wet heeft voldaan.

Van de vijf hierboven genoemde hoofdthema's luiden de belangrijkste bevindingen als volgt:

Autorisaties

Het autorisatieproces is onvoldoende op orde. De procedure voor het aanvragen van autorisaties wordt door de eenheden heel divers ingevuld. In één eenheid is een procedure aangetroffen voor het intrekken van autorisaties. In diverse eenheden ontbreken de autorisatiematrices of zijn deze niet actueel. Ten slotte constateert de ADR dat er geen gestructureerde controles worden uitgevoerd op de autorisaties.

Verstrekken

Hoewel er een landelijke procedure voor verstrekkingen van politiegegevens is opgesteld, is deze nog niet (volledig) binnen alle eenheden geïmplementeerd. Niet elk type verstrekking voldoet aan de vereisten uit de Wpg. Bij de verstrekkingen aan bijvoorbeeld de burgemeester en aan BOA's, wordt nog onvoldoende invulling gegeven aan de noodzakelijkheidstoets.

Protocolleren

De wet schrijft voor dat een aantal specifieke categorieën verwerkingen en de toekenning van autorisaties schriftelijk moet worden vastgelegd. Deze protocolplicht is bedoeld om intern en extern toezicht mogelijk te maken en om betrokkenen te informeren over wat er met hun gegevens is gedaan. De binnen de politie opgestelde protocolprocedure is nog niet in alle eenheden (volledig) geïmplementeerd. Ook de protocollering zelf gebeurt nog niet conform de Wpg.

Bewaartermijnen

De naleving van de bewaartermijnen is onvoldoende op orde. Dit komt mede doordat het verwijderen en vernietigen van gegevens uit diverse politiesystemen onvoldoende wordt ondersteund door de ICT. Medewerkers dienen hierdoor zelf schoningstermijnen in de gaten te houden en gegevens handmatig te verwijderen en te vernietigen, hetgeen, nog daargelaten de hiervoor vereiste discipline bij de tienduizenden politiemedewerkers, ook inhoudelijk geen sinecure is, aangezien bewaartermijnen van gegevens – afhankelijk van het type onderzoek – ook nog eens tussentijds kunnen veranderen. Wel is het zo dat de politie maatregelen getroffen heeft om te bewerkstelligen dat niet conform de wet vernietigde gegevens ontoegankelijk worden gemaakt. Het risico op een onrechtmatig gebruik van deze politiegegevens wordt daarmee geminimaliseerd.

Rechten van de betrokkene

Ook ten aanzien van dit onderwerp is een landelijke procedure opgesteld maar is deze nog niet binnen alle eenheden ingevoerd. De processtappen zoals kennisneming en verzoek om verbetering, aanvulling, verwijdering of afscherming zijn op dit moment nog onvoldoende op orde.

Uit de beoordeling van de overige zeven onderwerpen blijkt dat ook hier de naleving in meerdere of mindere mate niet op orde is. Ik verwijs hiervoor naar het bijgevoegde auditrapport.

Schengen Informatiesysteem (SIS-II) en Europees Visum Informatiesysteem (EUVIS)

Ook uit onderzoeken naar het Schengen Informatiesysteem en het Europees Visum Informatiesysteem zijn tekortkomingen met betrekking tot het naleven van informatiebeveiligings- en gegevensbeschermingsvoorschriften door de politie naar voren gekomen. Het CBP heeft als nationaal toezichthouder op het EU SIS(II)-Besluit onderzoek gedaan naar de vraag of de Nederlandse politie voldoende maatregelen heeft getroffen ter bescherming van de gegevens van het nationaal deel van het Schengen Informatiesysteem (N.SIS II). Tevens heeft de ADR een auditrapport opgesteld over de wijze waarop de beveiliging van het Europese Visum Informatiesysteem (EUVIS) door de politie is vormgegeven en of deze voldoet aan de verplichtingen uit het VIS-besluit. Deze audit vindt eens in de vier jaar plaats en is een verplichting uit de VIS-verordening. Uit de onderzoeken komen de volgende hoofdpunten naar voren.

Toepassing van het beveiligingsbeleid in de praktijk

De politie hanteert een eenduidig, generiek beleid voor de beveiliging van informatie. Dit beleid is van toepassing op alle systemen. Dit betekent dat geen specifiek plan is opgesteld voor de onderzochte systemen. Een

dergelijke generieke benadering is mogelijk, maar vereist in de toepassing uitwerking en in sommige gevallen maatwerk. De toepassing is echter onvoldoende uitgewerkt. Hierdoor kan onvoldoende worden vastgesteld of sprake is van een goede toepassing van dit beleid.

Toegangsrechten en personeelsprofielen/ Autorisatiebeheer

Het autorisatiebeheer bij de politie voldoet niet aan de eisen die vanuit wet- en regelgeving worden gesteld ten aanzien van de kwaliteit van autorisatiebeheer. Deze tekortkomingen zien op het niet procesmatig op orde hebben van het verstrekken, tussentijds controleren en intrekken van autorisaties. Dit beeld komt ook naar voren uit de audit Wpg.

Controle gebruik

Er is onvoldoende sprake van goede, interne, tussentijdse controle op onrechtmatig gebruik van de onderzochte systemen. Ook worden niet alle benodigde gegevens voor controle gelogd. Hierdoor ontstaat onvoldoende inzicht in en signalering van eventueel onrechtmatig gebruik.

Maatregelen

Het belang van een goede naleving van deze wetgeving is voor mij en voor de korpschef evident. Zoals ik eerder al opmerkte, zijn de samenleving en internationale partners zijn niet alleen gebaat bij een veilige en goede taakuitvoering door de politie, maar ook bij een zorgvuldige omgang met politiegegevens die voor die taakuitvoering noodzakelijk is. Veiligheid en het respecteren van de privacy zijn onlosmakelijk met elkaar verbonden.

De politie zal deze wetgeving structureel goed moeten gaan naleven. De korpschef zal het in de Wpg voorgeschreven verbeterplan aangrijpen om deze problemen aan te pakken. Realisme is daarbij op zijn plaats. Het zal jaren duren voordat alle genoemde knelpunten zullen zijn opgelost. Voor een goede naleving van de wet is een stevige basis noodzakelijk. Ik voorzie dat fundamentele wijzigingen in wetgeving en/of ICT-structuren nodig zijn om de uitvoerbaarheid van de wet te vergroten. Deze wijzigingen vragen tijd en zorgvuldigheid. Verder houd ik er rekening mee dat zich in de toekomst nieuwe problemen op dit gebied zullen openbaren, bijvoorbeeld als uitkomst van het in mijn brief van 30 oktober 2015 (naar aanleiding van de van corruptie verdachte politiemedewerker) aangekondigde inspectieonderzoek naar de opzet en werking van onder meer het autorisatiebeleid en het beleid om onjuist gebruik van politiesystemen tegen te gaan.

Een deel van de benodigde maatregelen is al in gang gezet. Ik doel hierbij in het bijzonder op de in mijn eerdergenoemde brief van 30 oktober 2015 vermelde realisatie van een landelijk autorisatiemodel voor toegang van politiefunctionarissen tot de politiesystemen. Uiterlijk eind 2016 zal het landelijk autorisatiemodel technisch zijn gerealiseerd. Vooruitlopend daarop heb ik steekproeven en de introductie van het «vier-ogen» principe aangekondigd. Ook de eerder toegezegde maatregelen die bijdragen aan het geautomatiseerd verwijderen en vernietigen van politiegegevens uit de twee meest gebruikte ICT-systemen (BVH en Summ-IT) zijn reeds in gang gezet.

Aanvullende maatregelen zijn echter nodig. Maatregelen die direct gericht zijn op het minimaliseren van de grootste risico's op schending van de persoonlijke levenssfeer en het ongeoorloofd gebruik van politiegegevens, zullen voorrang moeten krijgen. Het is onvermijdelijk dat een

aantal van deze maatregelen moet worden ingepast in de herijking van het realisatieplan voor de vorming van de nationale politie. Dit kan effecten hebben op de planning van andere onderdelen van de realisatie en het IV-portfolio. Van andere noodzakelijke maatregelen zal ik moeten accepteren dat deze niet op korte termijn kunnen worden verwezenlijkt. Voor deze categorie maatregelen zijn wijzigingen in de wet en/of structurele aanpassingen in de ICT-structuren noodzakelijk.

Het hierboven aangekondigde en door de Wpg voorgeschreven verbeterplan van de korpschef zal uiterlijk 1 maart 2016 gereed zijn. Ik verwacht van de korpschef een realistisch haalbaar verbeterplan dat tevens een ambitieus perspectief voor de toekomst biedt. Met de korpschef heb ik afgesproken dat het verbeterplan minimaal aan de volgende criteria voldoet:

- Op alle geconstateerde tekortkomingen moeten de noodzakelijke maatregelen worden uitgewerkt;
- Prioriteit moet worden gegeven aan maatregelen die nodig zijn om de grootste risico's op schending van de privacy te minimaliseren, waarbij het autorisatieproces, de informatiebeveiliging en rechten van betrokkenen voorrang zullen krijgen;
- Maatregelen die direct bijdragen aan een verbetering van de naleving hebben prioriteit boven maatregelen met een minder direct effect;
- De reeds ingezette maatregelen op gebied van het op orde brengen van de autorisaties en de maatregelen tot verbetering van de naleving van de bewaartermijnen maken onderdeel uit van het verbeterplan;
- In het verbeterplan wordt aangegeven hoe het generieke informatiebeveiligingsbeleid zo snel mogelijk en uniform in de hele organisatiepraktijk zal worden geïmplementeerd;
- In het verbeterplan wordt aangegeven welke specifieke maatregelen worden genomen ten aanzien van informatiebeveiliging en gegevensbescherming in N.SIS-II en EUVIS;
- Het verbeterplan is een meerjarenplan en bevat voor elke maatregel een duidelijk tijdpad;
- In het verbeterplan wordt ingegaan op de organisatorische inrichting die nodig is voor de effectieve uitvoering van het verbeterplan.
- In het verbeterplan wordt inzichtelijk gemaakt hoe de te nemen maatregelen worden ingepast in de meerjarenbegroting.

Binnen een jaar na oplevering van het verbeterplan zal de korpschef een hercontrole laten uitvoeren om te beoordelen of de korte-termijn-verbetermaatregelen effect hebben en op welke punten bijsturing noodzakelijk is. Gezien de omvang en de complexiteit van de noodzakelijke aanpassingen heb ik niet de verwachting dat de hercontrole en de toekomstige audits op korte termijn een geheel ander beeld zullen laten zien. De structurele problemen zullen moeten worden opgelost door aanpassingen van de wet, de bijbehorende implementatie en fundamentele wijzigingen in de ICT-structuren. Mede gelet op het herijkte realisatieplan zal dit de nodige tijd vergen.

De Minister van Veiligheid en Justitie,
G.A. van der Steur